

(19)日本国特許庁 (J P)

(12) 特 許 公 報 (B 2)

(11)特許番号

特許第3234202号  
(P3234202)

(45)発行日 平成13年12月4日(2001.12.4)

(24)登録日 平成13年9月21日(2001.9.21)

(51)Int.Cl.<sup>7</sup>

識別記号

F I

H 0 4 J 13/00

G 0 6 F 7/58

G 0 6 F 7/58

H 0 4 J 13/00

A

請求項の数17(全 11 頁)

(21)出願番号 特願平11-232312

(22)出願日 平成11年8月19日(1999.8.19)

(65)公開番号 特開2001-60937(P2001-60937A)

(43)公開日 平成13年3月6日(2001.3.6)

審査請求日 平成11年8月19日(1999.8.19)

(73)特許権者 301022471

独立行政法人通信総合研究所

東京都小金井市貫井北町4-2-1

(73)特許権者 597044841

梅野 健

東京都小金井市貫井北町4-2-1 独

立行政法人通信総合研究所内

(72)発明者 梅野 健

東京都小金井市貫井北町4丁目2番1号

郵政省通信総合研究所内

(74)代理人 100095407

弁理士 木村 満 (外1名)

審査官 北村 智彦

最終頁に続く

(54)【発明の名称】 擬似雑音系列の出力装置、送信装置、受信装置、通信システム、擬似雑音系列の出力方法、送信方法、受信方法、および、情報記録媒体

1

(57)【特許請求の範囲】

【請求項1】整数a ( $2 \leq a$ )についてのチェビシェフ多項式

$T(a, \cos \theta) = \cos(a\theta)$

により生成した長さN ( $1 \leq N$ )の擬似雑音系列を出力する擬似雑音系列の出力装置であって、

S ( $1 \leq S$ )個の-1より大きく1未満の実数の系列初期値

$x_1, x_2, \dots, x_S$

と、S個の2以上の整数の次数

$p_1, p_2, \dots, p_S$

と、を受け付ける受付部と、

前記受け付けられた系列初期値と次数と、整数j ( $1 \leq j$

$\leq S$ ), m ( $1 \leq m \leq N-1$ ), n ( $1 \leq n \leq N$ )についての漸化式

$x_1[1] = x_1$ ;

$x_1[m+1] = T(p_1, x_1[m])$ ;

2

$z[n] = \prod_{i=1}^S T(p_i, x_i[n])$

とにより、長さNの擬似雑音系列

$z[1], z[2], \dots, z[N]$

を計算する計算部と、

前記計算された擬似雑音系列を出力する出力部と、

を備えることを特徴とする擬似雑音系列の出力装置。

【請求項2】前記受け付けられる系列初期値はいずれも有理数であることを特徴とする請求項1に記載の擬似雑音系列の出力装置。

10 【請求項3】伝送信号の入力を受け付ける信号受付部と、

請求項1または2に記載の擬似雑音系列の出力装置に、

所定の系列初期値と、所定の次数と、を受け付けさせて

擬似雑音系列を出力させる系列出力部と、

前記受け付けられた伝送信号に、前記出力された擬似雑

音系列の要素を順に掛けて直接スペクトラム拡散する拡散部と、

前記直接スペクトラム拡散された信号を送信する送信部と、

を備えることを特徴とする送信装置。

【請求項4】請求項3に記載の送信装置により送信された信号を受信する信号受信部と、

請求項1または2に記載の擬似雑音系列の出力装置に、当該送信装置と同じ系列初期値と、当該送信装置と同じ次数と、を受け付けさせて擬似雑音系列を出力させる系列出力部と、

前記受信された信号に前記出力された擬似雑音系列の要素の逆数を順に掛けて直接スペクトラム逆拡散して当該送信装置が受け付けた伝送信号を復号する逆拡散部と、を備えることを特徴とする受信装置。

【請求項5】請求項3に記載の送信装置により送信された信号を受信する信号受信部と、

系列初期値、および、次数を生成する生成部と、

請求項1または2に記載の擬似雑音系列の出力装置に前記生成された系列初期値、および、次数を受け付けさせて擬似雑音系列を出力させる系列出力部と、

前記受信された信号に、前記出力された擬似雑音系列の要素を順に掛けて相関検波する相関検波部と、

前記相関検波の結果から、前記生成された系列初期値、および、次数が当該送信装置と同じ系列初期値、および、次数であると判断した場合、前記受信された信号に、前記相関検波により同期された擬似雑音系列の要素の逆数を順に掛けて直接スペクトラム逆拡散して当該送信装置が受け付けた伝送信号を復号する逆拡散部と、を備えることを特徴とする受信装置。

【請求項6】請求項3に記載の送信装置と、

請求項4または5に記載の受信装置であって、当該送信装置により送信された信号を受信する受信装置と、を備えることを特徴とする通信システム。

【請求項7】整数 $a$  ( $2 \leq a$ )についてのチェビシェフ多項式

$$T(a, \cos \theta) = \cos(a\theta)$$

により生成した長さ $N$  ( $1 \leq N$ )の擬似雑音系列を出力する擬似雑音系列の出力方法であって、

$S$  ( $1 \leq S$ )個の $-1$ より大きく $1$ 未満の実数の系列初期値

$$x_1, x_2, \dots, x_S$$

と、 $S$ 個の $2$ 以上の整数の次数

$$p_1, p_2, \dots, p_S$$

と、を受け付ける受付工程と、

前記受け付けられた系列初期値と次数と、整数 $j$  ( $1 \leq j \leq S$ ),  $m$  ( $1 \leq m \leq N-1$ ),  $n$  ( $1 \leq n \leq N$ )についての漸化式

$$x_1[1] = x_1;$$

$$x_1[m+1] = T(p_1, x_1[m]);$$

$$z[n] = \prod_{i=1}^S T(p_i, x_i[n])$$

とにより、長さ $N$ の擬似雑音系列

$$z[1], z[2], \dots, z[N]$$

を計算する計算工程と、

前記計算された擬似雑音系列を出力する出力工程と、

を備えることを特徴とする擬似雑音系列の出力方法。

【請求項8】前記受け付けられる系列初期値はいずれも有理数であることを特徴とする請求項7に記載の擬似雑音系列の出力方法。

【請求項9】伝送信号の入力を受け付ける信号受付工程と、

10 請求項7または8に記載の擬似雑音系列の出力方法に、所定の系列初期値と、所定の次数と、を受け付けさせて擬似雑音系列を出力させる系列出力工程と、

前記受け付けられた伝送信号に、前記出力された擬似雑音系列の要素を順に掛けて直接スペクトラム拡散する拡散工程と、

前記直接スペクトラム拡散された信号を送信する送信工程と、

を備えることを特徴とする送信方法。

【請求項10】信号を受信する信号受信工程と、

20 請求項7または8に記載の擬似雑音系列の出力方法に、所定の系列初期値と、所定の次数と、を受け付けさせて擬似雑音系列を出力させる系列出力工程と、

前記受信された信号に前記出力された擬似雑音系列の要素の逆数を順に掛けて直接スペクトラム逆拡散して伝送信号を復号する逆拡散工程と、

を備えることを特徴とする受信方法。

【請求項11】信号を受信する信号受信工程と、

系列初期値、および、次数を生成する生成工程と、

30 請求項7または8に記載の擬似雑音系列の出力方法に、前記生成された系列初期値、および、次数を受け付けさせて擬似雑音系列を出力させる系列出力工程と、

前記受信された信号に、前記出力された擬似雑音系列の要素を順に掛けて相関検波する相関検波工程と、

前記相関検波の結果から、前記生成された系列初期値、および、次数が所定の条件を満たすと判断した場合、前記受信された信号に、前記相関検波により同期された擬似雑音系列の要素の逆数を順に掛けて直接スペクトラム逆拡散して伝送信号を復号する逆拡散工程と、

を備えることを特徴とする受信方法。

40 【請求項12】整数 $a$  ( $2 \leq a$ )についてのチェビシェフ多項式

$$T(a, \cos \theta) = \cos(a\theta)$$

により生成した長さ $N$  ( $1 \leq N$ )の擬似雑音系列を出力する処理を実現するプログラムを記録したコンピュータ読取可能な情報記録媒体であって、前記プログラムは、

$S$  ( $1 \leq S$ )個の $-1$ より大きく $1$ 未満の実数の系列初期値

$$x_1, x_2, \dots, x_S$$

と、 $S$ 個の $2$ 以上の整数の次数

$$p_1, p_2, \dots, p_S$$

50 と、を受け付け、

前記受け付けられた系列初期値と次数と、整数 $j$  ( $1 \leq j \leq S$ ),  $m$  ( $1 \leq m \leq N-1$ ),  $n$  ( $1 \leq n \leq N$ )についての漸化式

$$x_i[1] = x_i;$$

$$x_i[m+1] = T(p_i, x_i[m]);$$

$$z[n] = \prod_{i=1}^S T(p_i, x_i[n])$$

とにより、長さ $N$ の擬似雑音系列

$$z[1], z[2], \dots, z[N]$$

を計算し、

前記計算された擬似雑音系列を出力する処理を実現することを特徴とする情報記録媒体。

【請求項13】前記受け付けられる系列初期値はいずれも有理数であることを特徴とする請求項12に記載の情報記録媒体。

【請求項14】伝送信号の入力を受け付け、請求項12または13に記載の情報記録媒体に記録されたプログラムに、所定の系列初期値と、所定の次数と、を受け付けさせて擬似雑音系列を出力させ、前記受け付けられた伝送信号に、前記出力された擬似雑音系列の要素を順に乗じて直接スペクトラム拡散し、前記直接スペクトラム拡散された信号を送信する処理を実現するプログラムを記録したコンピュータ読取可能な情報記録媒体。

【請求項15】信号を受信し、請求項12または13に記載の情報記録媒体に記録されたプログラムに、所定の系列初期値と、所定の次数と、を受け付けさせて擬似雑音系列を出力させ、前記受信された信号に前記出力された擬似雑音系列の要素の逆数を順に乗じて直接スペクトラム逆拡散して伝送信号を復号する処理を実現するプログラムを記録したコンピュータ読取可能な情報記録媒体。

【請求項16】信号を受信し、系列初期値、および、次数を生成し、請求項12または13に記載の情報記録媒体に記録されたプログラムに、前記生成された系列初期値、および、次数を受け付けさせて擬似雑音系列を出力させ、前記受信された信号に、前記出力された擬似雑音系列の要素を順に乗じて相関検波し、前記相関検波の結果から、前記生成された系列初期値、および、次数が所定の条件を満たすと判断した場合、前記受信された信号に、前記相関検波により同期された擬似雑音系列の要素の逆数を順に乗じて直接スペクトラム逆拡散して伝送信号を復号する処理を実現するプログラムを記録したコンピュータ読取可能な情報記録媒体。

【請求項17】前記情報記録媒体は、コンパクトディスク、フロッピー（登録商標）ディスク、ハードディスク、光磁気ディスク、デジタルビデオディスク、磁気テープ、または、半導体メモリであることを特徴とする請求項12から16に記載の情報記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、PN (Pseudorandom Noise; 擬似雑音) 系列の出力装置、送信装置、受信装置、通信システム、PN系列の出力方法、送信方法、受信方法、および、情報記録媒体に関する。

【0002】特に、衛星通信、固定通信、携帯電話やPHS (Personal Handyphone System) などの陸上移動通信、GPS (Global Positioning System) などの測距分野で用いることができるスペクトラム拡散通信のCDMA (Code Division Multiple Access; 符号分割多元接続) 方式の拡散符号として使用できるPN系列を出力するのに好適な出力装置、出力方法と、これを用いた送信装置、受信装置、通信システム、送信方法、受信方法、および、情報記録媒体に関する。

【0003】

【従来の技術】CDMA方式を用いるスペクトラム拡散通信などでは、PN系列を拡散符号として用いることにより、秘話性を高くし、帯域の利用効率をあげている。

【0004】従来、PN系列としては、M系列、Gold符号、高符号などが利用されていた。これらの系列は、シフトレジスタやこれと排他的論理和回路を組み合わせることにより計算することができるが、2値系列を基本とするため、通信セキュリティを確保することが難しかった。

【0005】一方で、スペクトラム拡散通信では、通信を行う端末の間で同期をとる必要があるが、通信セキュリティを高めることと同期を容易に行うこととは互いにトレードオフの関係にある。

【0006】

【発明が解決しようとする課題】しかしながら、これら従来のPN系列よりもさらに秘話性を高めることができるPN系列を出力する手法が産業界から望まれている。特に、近年発展が目覚ましいカオス理論に基づいて、同定の難しいPN系列を出力し、これをCDMA方式の拡散符号として用いてスペクトラム拡散通信の秘話性を高める手法に対する要望は大きい。

【0007】一方、カオス理論に基づいたPN系列を単純に用いるのでは、通信の受信側で同期をとる際に、拡散符号をサーチすべき空間が莫大になるため、同期を容易に行う手法が望まれている。

【0008】本発明は、以上のような問題を解決するためになされたもので、本発明は、PN (Pseudorandom Noise; 擬似雑音) 系列の出力装置、送信装置、受信装置、通信システム、PN系列の出力方法、送信方法、受信方法、および、情報記録媒体を提供することを目的とする。

【0009】特に、スペクトラム拡散通信のCDMA方式の拡散符号として使用できるPN系列を出力するのに好適な出力装置、出力方法と、これを用いた送信装置、受信装置、通信システム、送信方法、受信方法、および、情報記録媒体を提供することを目的とする。

【0010】

【課題を解決するための手段】以上の目的を達成するため、本発明の原理にしたがって、下記の発明を開示する。

【0011】本発明のPN系列の出力装置は、整数 $a$  ( $2 \leq a$ )についてのチェビシェフ多項式

$$T(a, \cos \theta) = \cos(a\theta)$$

により生成した長さ $N$  ( $1 \leq N$ )のPN系列を出力するPN系列の出力装置であり、受付部と、計算部と、出力部と、を備えるように構成する。

【0012】受付部は、 $S$  ( $1 \leq S$ )個の $-1$ より大きく $1$ 未満の実数の系列初期値

$$x_1, x_2, \dots, x_S$$

と、 $S$ 個の $2$ 以上の整数の次数

$$p_1, p_2, \dots, p_S$$

と、を受け付ける。

【0013】計算部は、受け付けられた系列初期値と次数と、整数 $j$  ( $1 \leq j \leq S$ )、 $m$  ( $1 \leq m \leq N-1$ )、 $n$  ( $1 \leq n \leq N$ )についての漸化式

$$x_i[1] = x_i;$$

$$x_i[m+1] = T(p_i, x_i[m]);$$

$$z[n] = \prod_{i=1}^S T(p_i, x_i[n])$$

とにより、長さ $N$ のPN系列

$$z[1], z[2], \dots, z[N]$$

を計算する。

【0014】出力部は、計算されたPN系列を出力する。

【0015】また、本発明のPN系列の出力装置において受け付けられる系列初期値はいずれも有理数であるように構成することができる。

【0016】本発明の送信装置は、信号受付部と、系列出力部と、拡散部と、送信部と、を備えるように構成する。

【0017】信号受付部は、伝送信号の入力を受け付ける。

【0018】系列出力部は、上記のPN系列の出力装置に、所定の系列初期値と、所定の次数と、を受け付けさせてPN系列を出力させる。

【0019】拡散部は、受け付けられた伝送信号に、出力されたPN系列の要素を順に乗じて直接スペクトラム拡散する。

【0020】送信部は、直接スペクトラム拡散された信号を送信する。

【0021】本発明の受信装置は、信号受付部と、系列出力部と、逆拡散部と、を備えるように構成する。

【0022】信号受付部は、上記の送信装置により送信された信号を受信する。

【0023】系列出力部は、上記のPN系列の出力装置に、当該送信装置と同じ系列初期値と、当該送信装置と同じ次数と、を受け付けさせてPN系列を出力させる。

【0024】逆拡散部は、受信された信号に出力された

PN系列の要素の逆数を順に乗じて直接スペクトラム逆拡散して当該送信装置が受け付けた伝送信号を復号する。

【0025】本発明の受信装置は、信号受付部と、生成部と、系列出力部と、相関検波部と、逆拡散部と、を備えるように構成する。

【0026】信号受付部は、上記の送信装置により送信された信号を受信する。

【0027】生成部は、系列初期値、および、次数を生成する。

【0028】系列出力部は、生成された系列初期値、および、次数を、上記のPN系列の出力装置に受け付けさせてPN系列を出力させる。

【0029】相関検波部は、受信された信号に、出力されたPN系列の要素を順に乗じて相関検波する。

【0030】逆拡散部は、相関検波の結果から、生成された系列初期値、および、次数が当該送信装置と同じ系列初期値、および、次数であると判断した場合、受信された信号に、相関検波により同期されたPN系列の要素の逆数を順に乗じて直接スペクトラム逆拡散して当該送信装置が受け付けた伝送信号を復号する。

【0031】本発明の通信システムは、上記の送信装置と、上記の受信装置であって、当該送信装置により送信された信号を受信する受信装置と、を備えるように構成する。

【0032】本発明のPN系列の出力方法は、整数 $a$  ( $2 \leq a$ )についてのチェビシェフ多項式

$$T(a, \cos \theta) = \cos(a\theta)$$

により生成した長さ $N$  ( $1 \leq N$ )のPN系列を出力するPN系列の出力方法であって、受付工程と、計算工程と、出力工程と、を備えるように構成する。

【0033】受付工程にて、 $S$  ( $1 \leq S$ )個の $-1$ より大きく $1$ 未満の実数の系列初期値

$$x_1, x_2, \dots, x_S$$

と、 $S$ 個の $2$ 以上の整数の次数

$$p_1, p_2, \dots, p_S$$

と、を受け付ける。

【0034】計算工程にて、受け付けられた系列初期値と次数と、整数 $j$  ( $1 \leq j \leq S$ )、 $m$  ( $1 \leq m \leq N-1$ )、 $n$  ( $1 \leq n \leq N$ )についての漸化式

$$x_i[1] = x_i;$$

$$x_i[m+1] = T(p_i, x_i[m]);$$

$$z[n] = \prod_{i=1}^S T(p_i, x_i[n])$$

とにより、長さ $N$ のPN系列

$$z[1], z[2], \dots, z[N]$$

を計算する。

【0035】出力工程にて、計算されたPN系列を出力する。

【0036】また、本発明のPN系列の出力方法において、受け付けられる系列初期値はいずれも有理数である

ように構成することができる。

【0037】本発明の送信方法は、信号受付工程と、系列出力工程と、拡散工程と、送信工程と、を備えるように構成する。

【0038】信号受付工程は、伝送信号の入力を受け付ける。

【0039】系列出力工程は、上記のPN系列の出力方法に、所定の系列初期値と、所定の次数と、を受け付けてさせてPN系列を出力させる。

【0040】拡散工程は、受け付けられた伝送信号に、出力されたPN系列の要素を順に乗じて直接スペクトラム拡散する。

【0041】送信工程は、直接スペクトラム拡散された信号を送信する。

【0042】本発明の受信方法は、信号受信工程と、系列出力工程と、逆拡散工程と、を備えるように構成する。

【0043】信号受信工程にて、信号を受信する。

【0044】系列出力工程にて、上記のPN系列の出力方法に、所定の系列初期値と、所定の次数と、を受け付けてさせてPN系列を出力させる。

【0045】逆拡散工程にて、受信された信号に出力されたPN系列の要素の逆数を順に乗じて直接スペクトラム逆拡散して伝送信号を復号する。

【0046】本発明の受信方法は、信号受信工程と、生成工程と、系列出力工程と、逆拡散工程と、を備えるように構成する。

【0047】信号受信工程にて、信号を受信する。

【0048】生成工程にて、系列初期値、および、次数を生成する。

【0049】系列出力工程にて、上記のPN系列の出力方法に、生成された系列初期値、および、次数を受け付けてさせてPN系列を出力させる。

【0050】相関検波工程にて、受信された信号に、出力されたPN系列の要素を順に乗じて相関検波する。

【0051】逆拡散工程にて、相関検波の結果から、生成された系列初期値、および、次数が所定の条件を満たすと判断した場合、受信された信号に、相関検波により同期されたPN系列の要素の逆数を順に乗じて直接スペクトラム逆拡散して伝送信号を復号する。

【0052】本発明のPN系列の出力装置、送信装置、受信装置、通信システムにて実行される処理と、PN系列の出力方法、送信方法、および、受信方法と、を実現するプログラムをコンパクトディスク、フロッピーディスク、ハードディスク、光磁気ディスク、デジタルビデオディスク、磁気テープ、半導体メモリなどの情報記録媒体に記録することができる。

【0053】本発明の情報記録媒体に記録されたプログラムを、記憶装置、計算装置、出力装置、通信装置などを備える汎用コンピュータ、携帯電話機、PHS装置、

ゲーム装置などの携帯端末、並列計算機などの情報処理装置などで実行することにより、上記のPN系列の出力装置、送信装置、受信装置、通信システムにて実行される処理と、PN系列の出力方法、送信方法、および、受信方法と、を実現することができる。

【0054】また、情報処理装置とは独立して、本発明のプログラムを記録した情報記録媒体を配布、販売することができる。

【0055】

10 【発明の実施の形態】以下に本発明の一実施形態を説明する。なお、以下に説明する実施形態は説明のためのものであり、本願発明の範囲を制限するものではない。したがって、当業者であればこれらの各要素もしくは全要素をこれと均等なものに置換した実施形態を採用することが可能であるが、これらの実施形態も本願発明の範囲に含まれる。

【0056】(PN系列の出力装置の実施形態)図1は、本発明のPN系列の出力装置の概要構成を示す模式図(データフロー図)である。以下、図1を参照して説明する。

【0057】PN系列の出力装置101は、受付部102と、計算部103と、出力部104と、を備える。

【0058】受付部102は、 $S$  ( $1 \leq S$ )個の実数の系列初期値 $x_1, x_2, \dots, x_S$ と、 $S$ 個の整数の次数 $p_1, p_2, \dots, p_S$ と、を受け付ける。これらは、整数 $j$  ( $1 \leq j \leq S$ )について、条件 $-1 < x_j < 1$ ,  $2 \leq p_j$ を満たす必要がある。

30 【0059】計算部103は、受付部102が受け付けた系列初期値と次数と、チェビシェフ多項式を用いて、長さ $N$  ( $1 \leq N$ )の擬似雑音系列 $z[1], z[2], \dots, z[N]$ を生成する。出力部104は、計算部103が生成した擬似雑音系列を出力する。

【0060】図2は、チェビシェフ多項式を表したグラフである。チェビシェフ多項式は、整数 $a$ を次数とするとき、

$$T(a, \cos \theta) = \cos(a\theta)$$

のように、余弦関数の加法定理により定義することができる。

40 【0061】一方、以下のように、有理多項式で直接表現することもできる。

$$T(2, x) = 1 - x^2$$

$$T(3, x) = 4x^3 - 3x$$

チェビシェフ多項式 $y = T(a, x)$ は、いずれも、開区間 $-1 < x < 1$ を開区間 $-1 < y < 1$ に写像する有理写像である。

【0062】図2には、次数2から5のチェビシェフ多項式が、 $y = T(2, x)$ ,  $y = T(3, x)$ ,  $y = T(4, x)$ ,  $y = T(5, x)$ の形式でグラフ表示されている。横軸が $x$ 軸、縦軸が $y$ 軸である。

50 【0063】計算部103の計算は、コンピュータによる多項式演算により実現することができるほか、加減算

回路と乗算回路の組合せによっても実現できる。また、所定の精度保証をした浮動小数点演算で実現してもよいし、有理数による演算により実現することもできる。

【0064】また、受付部102における系列初期値および次数の受け付けや、出力部104における出力は、コンピュータの場合にはRAM(Random Access Memory)やCPU(Central Processing Unit: 中央処理ユニット)内のレジスタを介して行うことができ、電子回路の場合には、ラッチなどを用いて実現することができる。

【0065】なお、このようなチェビシェフ多項式に基づいて生成したPN系列そのものをCDMA方式の拡散符号として用いた場合、相関関数がほぼ直交し、相関特性が、従来のM系列、Gold符号、高符号と比較して良好であることが、発明者らによって発見されている

(文献1: K. Umeno and K. Kitayama, Electronics Letters (1999) Vol. 35, pp.545-546; 文献2: K. Umeno and K. Kitayama, to appear in Proc. 1999, IEEE Information Theory Workshop, p. 106)。本発明において生成する擬似雑音系列も、これと同様の性質を有することが、相関関数を2次元の多重積分の形で表す文献2の手法により証明できる。

【0066】計算部103における計算は、整数 $j$  ( $1 \leq j \leq S$ ),  $m$  ( $1 \leq m \leq N-1$ ),  $n$  ( $1 \leq n \leq N$ )についての漸化式

$$x_i[1] = x_i;$$

$$x_i[m+1] = T(p_i, x_i[m]);$$

$$z[n] = \prod_{i=1}^S T(p_i, x_i[n])$$

に基づいて行われる。

【0067】ここで、 $\Pi$ は、数学の分野で $\Sigma$ と同様に一般的に用いられる演算を意味する。これらは、以下のよう

$$\sum_{i=1}^S a_i = a_1 + a_2 + \dots + a_S$$

$$\prod_{i=1}^S a_i = a_1 \times a_2 \times \dots \times a_S$$

【0068】上記の漸化式を見れば明らかなように、 $z[1], z[2], \dots, z[N]$ をそれぞれ求めるための計算は互いに独立しているため、並列度最大 $N$ で並列に計算を行うことができる。また、漸化式で記述されているため、ループによる繰り返し演算によっても容易に計算を行うことができる。

【0069】図3は、PN系列の出力装置101において実行される処理、すなわち、本発明のPN系列の出力方法の工程を示すフローチャートである。PN系列の出力装置101は、系列初期値と次数を受け付け(ステップS301)、これらと上記の漸化式に基づいてPN系列を計算し(ステップS302)、計算したPN系列を出力して(ステップS303)、本処理を終わる。

【0070】このように、本発明のPN系列の出力方法は、汎用コンピュータ、並列コンピュータ、携帯端末、特に通信端末、ゲーム装置などの情報処理装置により容易に実行することができる。

【0071】(送信装置の実施形態)図4は、本発明の送信装置の概要構成を示す模式図である。なお、図1と同じ要素には、同じ符号を付してある。以下、図4を参照して説明する。

【0072】送信装置401は、信号受付部402と系列出力部403と、拡散部404と、信号送信部405と、を備える。系列出力部403は、PN系列の出力装置101を備えており、これを制御する。

【0073】信号受付部402は、伝送すべき信号を受け付ける。伝送信号として典型的なものは、携帯電話やPHSの場合には音声信号である。デジタル通信を行う場合には電気的なデジタル信号である。光通信を行う場合には、光信号から電気信号への変換を行った上で電気信号を受け付けてもよいし、PN系列の出力装置101を光コンピュータで実現する場合は、光信号をそのまま受け付ける。

【0074】系列出力部403は、送信装置401に割り当てられた系列初期値と次数とを、これが備えるPN系列の出力装置101に受け付けさせる。PN系列の出力装置101は、上述のように、PN系列を出力するので、系列出力部403は、このPN系列を出力する。

【0075】系列初期値と次数とは、送信装置401のそれぞれに異なる値をあらかじめ割り当てることができる。製造番号、機器番号、承認番号などの数値をROM(Read Only Memory)に記録した通信端末が普及しているが、これと同様に、系列初期値と次数とをあらかじめROMに記録しておいて、当該送信装置401が常に同じ系列初期値と次数とを用いるようにすることができる。また、ROM内に使用する系列初期値と次数とを複数の種類記録しておき、これらを通信ごとにランダムに選択する手法も利用できる。

【0076】このような実施形態をとる場合、送信装置401と通信する受信装置では、ROM内に記録された系列初期値と次数とを何らかの方法で知る必要があるが、送信装置と受信装置とが1対になっている場合には、同じ系列初期値と次数とを共有して記録する実施形態をとることができる。

【0077】系列初期値と次数の種類が複数ある場合に、送信装置がいずれを使用しているか、は、後述する相関検波によって調べることができる。また、チェビシェフ多項式に基づく漸化式によって得られるカオス乱数列を用いて系列初期値を複数用意してもよい。さらに、後述するように、公開鍵暗号の手法を用いて、送信装置401と受信装置とで系列初期値と次数を安全に共有することができる。

【0078】拡散部404は、信号受付部402が受け付けた伝送信号に、系列出力部403が出力したPN系列の要素を順に乗じて直接スペクトラム拡散する。ここで、時刻 $t$ における信号の値を $s(t)$ として、「信号 $s(t)$ に系列の要素を順に乗じる」手法について説明する。

【0079】長さ $N$ の系列の要素を用いる場合には、これと直接スペクトラム拡散のチップ長 $w$ から、「信号 $s(t)$ に系列の要素を順に乘じる」の周期は、 $Nw$ になる。

【0080】所定の時刻 $t_0$ から「信号 $s(t)$ に系列の要素を順に乘じる」場合、信号 $s(t)$ を、必要な品質が得られるようなチップ長 $w$ で離散化する。たとえば、チップ長 $w$ ごとに信号 $s(t)$ の値を得る手法や、チップ長 $w$ の間の信号 $s(t)$ の値の平均を得る手法などが考えられる。ここでは、説明を明確にするため、前者の手法を用いて説明する。

【0081】チップ長 $w$ は、受信装置側で伝送信号の情報を十分に必要の品質で復号できるような長さにする必要があるが、公知の技法により、適切なチップ長を選択することができる。

【0082】また、適切なチップ長 $w$ を選択すれば、離散化された信号列を順に当該チップ長時間 $w$ だけ出力することにより、元の伝送信号から見て十分な品質の信号を得ることができる。

【0083】離散化された信号は、以下のような数列で表現することができる。

$s(t_0), s(t_0+w), s(t_0+2w), s(t_0+3w), s(t_0+4w), \dots$

【0084】これは、整数 $i$  ( $0 \leq i$ )について

$s_i = s(t_0 + iw)$

と整理することができる。なお、チップ長 $w$ の間の信号 $s(t)$ の値の平均をとる手法では、以下のように整理することができる。

$s_i = (1/w) \int_{t_0 + (i-1)w}^{t_0 + iw} s(t) dt$

【0085】これらの信号列 $s_i$  ( $0 \leq i$ )は、必要な品質で伝送信号を離散化したものである。

【0086】この信号列を、直接スペクトラム拡散した後の信号列は、

$s_0 z[1], s_1 z[2], \dots, s_{N-1} z[N], s_N z[1], s_{N+1} z[2],$

$\dots$

ようになる。すなわち、整数 $i$  ( $0 \leq i$ )に対して、 $s_i z[(i \bmod N) + 1]$ が、この数列の一般項である。ここで、 $x \bmod y$ は、 $x$ を $y$ で割った余りを意味する。

【0087】この信号列の要素を、それぞれチップ長の時間だけ送信することにより、受け付けられた所定の時間長の伝送信号を同じ時間長で送信することができる。

図5には、直接スペクトラム拡散処理の様子を示す。信号受付部402が受け付けた伝送信号501に対して、系列出力部403が出力したPN系列502の要素を繰り返し乗ずることにより、拡散部404が出力する信号503が得られる。

【0088】信号送信部405は拡散部404が出力する信号503を送信する。送信は、たとえば、携帯電話やPHSの場合はアンテナを介して、コンピュータ通信網の場合は有線の電話回線や有線/無線LAN回線を介して、あるいは光ケーブルを介して行われる。

【0089】(受信装置の実施形態) 本発明の受信装置

は、上記の送信装置同様、上記のPN系列の出力装置を用いてPN系列を得て、これを直接スペクトラム逆拡散用の拡散符号として用いる。図6は、本発明の受信装置の概要構成を示す模式図である。以下、図6を参照して説明する。

【0090】受信装置601は、信号受信部602と、系列出力部604と、逆拡散部605と、を備える。

【0091】信号受信部602は、上記の送信装置401により送信された信号を受信する。信号受信部602は、たとえば、アンテナ、電話回線や光ケーブル回線などに対するインターフェースにより実現される。

【0092】信号受信部602が受信する信号には、通信相手以外の送信装置401が送信した信号や、ノイズが含まれている。これら不要な信号を除去するために、通信相手の送信装置401が直接スペクトラム拡散に用いたPN系列と同じPN系列を用いる。系列出力部604は、通信相手の送信装置401が用いた系列初期値と次数と、を上記のPN系列の出力装置101に受け付けさせることにより、このPN系列を出力する。したがって、受信装置601の系列出力部604の実施態様は、送信装置401の系列出力部403と同様である。

【0093】通信相手の送信装置401が受け付けた伝送信号を復号するには、通信相手の送信装置401が送信した信号に対して、PN系列の要素の逆数を順に乘じて直接スペクトラム逆拡散すればよい。同期が取れていれば、受信した信号列

$s_0 z[1], s_1 z[2], \dots, s_{N-1} z[N], s_N z[1], s_{N+1} z[2],$

$\dots$

に、PN系列の要素の逆数

$1/z[1], 1/z[2], \dots, 1/z[N]$

を順に乘ずることにより、伝送信号の情報を必要な品質で復号した信号列

$s_0, s_1, \dots, s_{N-1}, s_N, s_{N+1}, \dots$

が得られる。この信号列を、それぞれチップ長時間 $w$ だけ順に出力すれば、伝送信号が必要な品質で復元できるのである。

【0094】同期には、後述する相関検波のほか、クロックを共有する手法など、各種の手法が考えられ、これらの実施形態も本発明の範囲に含まれる。

【0095】送信装置401と受信装置601とで通信を行う公開鍵暗号の手法を用いて、生成部611は、送信装置401と同じ系列初期値および次数を生成することができる。

【0096】まず、受信装置601は、公開鍵と秘密鍵の対を生成する。次に、受信装置601は、送信装置401に対して公開鍵を送信する。送信装置は、自ら使用する系列初期値および次数を当該公開鍵で暗号化して受信装置601に送信する。受信装置601は、送られた暗号を秘密鍵で復号し、系列初期値および次数を得る。

【0097】このような公開鍵暗号の手法として、本発

明の発明者が特願平11-152063号に開示するようなカオス暗号を用いることができる。

【0098】(相関検波の実施形態) 送信装置401で複数のPN系列からいずれかを選択して直接スペクトラム拡散した場合、受信装置601は、相関検波により、選択されたPN系列を知得することができる。また、相関検波により、直接スペクトラム逆拡散のための同期をとることができる。以下、図7を参照して、相関検波を行う場合の受信装置の実施形態について説明する。なお、図7では、図6に示す要素と同じものには同じ符号を付している。

【0099】受信装置601は、信号受信部602と、系列出力部604と、逆拡散部605と、のほか、生成部611と、相関検波部612を備える。

【0100】生成部611は、送信装置401で選択可能な系列初期値と次数の組を出力する。PN系列を1つだけ出力してもよい。この場合、相関検波部612は、複数の系列初期値と次数の組からいずれか1つの組を選択する必要はないため、信号の同期をとるために機能する。

【0101】系列出力部604は、生成部611が生成する系列初期値と次数に応じて、送信装置401で選択可能なPN系列をそれぞれ出力する。

【0102】相関検波部612では、系列出力部604が出力するPN系列のそれぞれについて相関検波を試みる。調べたいPN系列の「要素」を順に受信した信号に乗ずることにより、相関検波を行う。相関検波の手法については公知の技法を用いることができる。

【0103】本発明で用いるPN系列は、相関特性に優れているため、受信装置で異なるPN系列を選択した場合には、乗じた後の信号の強度が極めて弱くなり、相関検波に失敗する。

【0104】一方、送信装置のPN系列と同じものを選択して相関検波を行った場合は、乗じた後の信号の強度が所定の値を超えることになる。また、受信信号に同期するようにPN系列のオフセットを移動して信号の同期をとることができる。

【0105】逆拡散部605は、信号受信部602により受信された信号に、相関検波部612により選択されて当該受信された信号に同期されたPN系列の「要素の逆数」を順に乗じて、伝送信号を復号する。

【0106】受信された信号に対して、相関検波部612ではPN系列の「要素」を順に乗ずるのに対し、逆拡散部605ではPN系列の「要素の逆数」を順に乗ずる点異なる。前者では、自己相関、相互相関を計算するのに対し、後者では、復号が行われるのである。

【0107】(通信システム) 本発明の通信システムは、上記の送信装置401と、これが送信する信号を受信して伝送信号を復号する上記の受信装置601と、から構成することができる。これらの送信装置401と受

信装置601で、使用するPN系列が異なれば伝送信号の復号に失敗する。

【0108】したがって、複数の送信装置401と複数の受信装置601と同じ周波数帯で通信していても、秘話性を保つとともに、使用している通信者の対の数に応じた品質を保証して、相互に通信を行うことができる。

【0109】特に、本発明にて生成されるPN系列では、従来のPN系列に比較して符号の種類を格段に増やすことができるため、潜在的に多数のユーザを含むようなCDMA方式の通信に適している。

【0110】

【発明の効果】以上説明したように、本発明によれば、PN系列の出力装置、送信装置、受信装置、通信システム、PN系列の出力方法、送信方法、受信方法、および、情報記録媒体を提供することができる。

【0111】特に、スペクトラム拡散通信のCDMA方式の拡散符号として使用でき、秘話性の高いPN系列を出力するのに好適な出力装置、出力方法と、これを用いた送信装置、受信装置、通信システム、送信方法、受信方法、および、情報記録媒体を提供することができる。

【図面の簡単な説明】

【図1】本発明のPN系列の出力装置の実施形態の概要構成を示す模式図である。

【図2】チェビシェフ多項式の様子を示すグラフである。

【図3】本発明のPN系列の出力方法の工程を示すフローチャートである。

【図4】本発明の送信装置の概要構成を示す模式図である。

【図5】本発明の送信装置による直接スペクトラム拡散の様子を示す説明図である。

【図6】本発明の受信装置の概要構成を示す模式図である。

【図7】本発明の受信装置の概要構成を示す模式図である。

【符号の説明】

101 PN系列の出力装置

102 受付部

103 計算部

104 出力部

401 送信装置

402 信号受付部

403 系列出力部

404 拡散部

405 信号送信部

501 伝送信号

502 PN系列

503 出力信号

601 受信装置

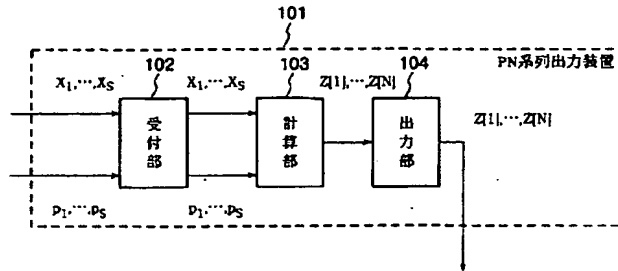


602 信号受信部  
604 系列出力部  
605 逆拡散部

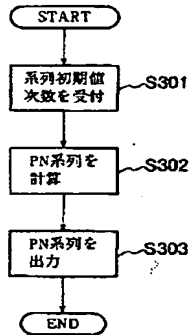
\*611 生成部  
612 相関検波部

\*

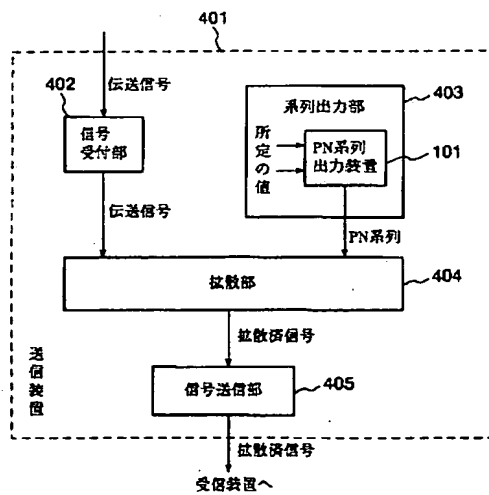
【図1】



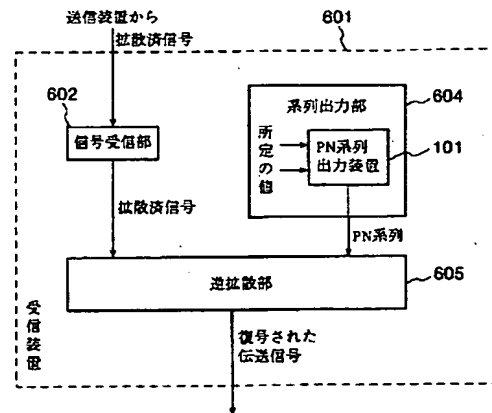
【図3】



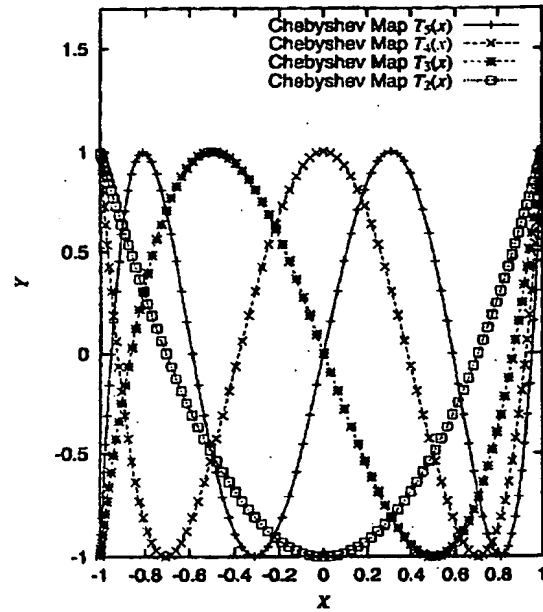
【図4】



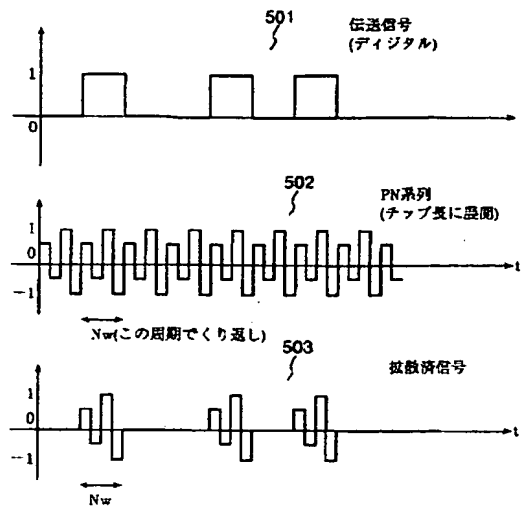
【図6】



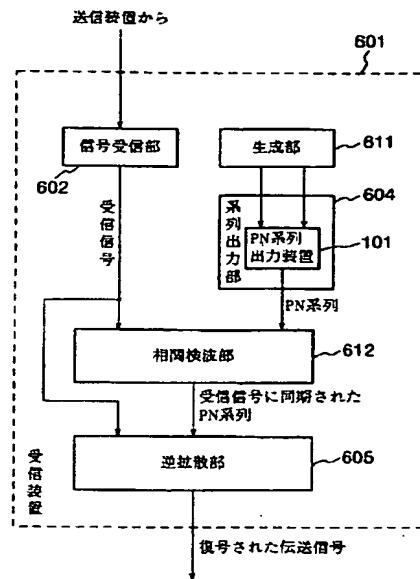
【図2】



【図5】



【図7】



## フロントページの続き

- (56)参考文献 特開2000-338869 (J P, A)  
 特開 平11-266179 (J P, A)  
 特開2000-276331 (J P, A)  
 香田徹, 常田明夫, 一ノ宮英俊, S S  
 通信の拡散符号としての有限周期カオス  
 2進系列の相関特性, 電子情報通信学会  
 技術研究報告, 1993年3月17日, V o  
 l. 92, No. 507, S S T 92-74, p.  
 7-12  
 梅野健, 北山研一, カオス符号を用い  
 たC D M Aの理論解析: 最良2値P N系  
 列との比較, 1999年電子情報通信学会総  
 合大会講演論文集, 1999年3月8日, 基  
 礎・境界, p. 508-509  
 香田徹, 常田明夫, 一ノ宮英俊, 松藤  
 信哉, 2値系列の偶および奇周期相関関  
 数の差異について, 1994年電子情報通信  
 学会春季大会講演論文集, 1994年3月10  
 日, 基礎・境界, p. 1-263  
 K. Umenô, K. Kitayam  
 a, Spreading sequen  
 ces using periodic  
 orbits of chaos f  
 or CDMA, ELECTRONIC  
 S LETTERS, 1999年4月1日,  
 Vol. 35, No. 7, p. 545-546

(58)調査した分野(Int.Cl.<sup>7</sup>, D B名)

H04B 1/69 - 1/713  
 H04J 13/00 - 13/06  
 G06F 7/58  
 J I C S Tファイル (J O I S)